学校编码：10384　　分类号_____密级_____
学号：X2011230434　　UDC _____

厦门大学

工 程 硕 士 学 位 论 文

金融 IC 卡的行业应用研究与设计

Research and Design of Industry Application of Financial IC Card

陈杰

指 导 教 师： 董 槐 林 教 授

专 业 名 称： 软 件 工 程

论文提交日期： 2013 年 4 月

论文答辩日期： 2013 年 5 月

学位授予日期： 年 月

指 导 教 师：_____

答辩委员会主席：_____

2013 年 4 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为某商业银行省分行金融 IC 卡行业应用与研究课题组的研究成果，在某商业银行省分行软件开发测试中心完成。

声明人（签名）：

2013 年　月　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　√　）2.不保密，适用上述授权。

声明人（签名）：

2013 年　　月　　日

摘　要

金融 IC 卡是金融信息化的产物。随着 IC 卡技术的成熟和金融行业标准的规范，IC 卡的安全性、便捷性、多应用性得到广泛认可，国内外各种 IC 卡应用发展迅猛，金融系统的服务与行业需求的对接成为一种现实的和必然的要求，金融 IC 卡系统的技术研究和应用也成为一种必然趋势。

商业银行面对紧迫的行业压力、旺盛的市场需求、激烈的同业竞争，开发金融 IC 卡行业运用平台。本文依据某商业银行金融 IC 卡信息系统开发项目，围绕系统需求分析、系统构架设计和系统功能设计完成课题设计，阐述了金融 IC 卡的行业应用研究和设计。

本项目基于 Tuxedo 中间件开发，使用 Oracle 数据库，采用统一建模语言(UML)为需求分析和设计描述语言，运用自上而下、层层细化的方法，采用分层设计、规范接口、预留技术冗余方便扩展的方式，实现了前置终端管理、IC 卡管理、电子钱包、脱机消费、日终账务处理、报表统计、密钥安全管理等功能。

该系统以标准化接口和应用流程，全面整合了该行现有 IC 卡业务，很好地解决与银行现有系统、现有业务的接入与融合，为银行卡从磁条卡过渡到 IC 卡提供有力的支持保障，同时为基于金融 IC 卡的行业应用拓展提供坚实的基础。

本文从国内外金融 IC 卡发展运用趋势和银行卡发展现状、提高用卡安全性和满足金融 IC 卡行业应用为出发点，详细论述了某商业银行金融 IC 卡项目系统开发实现中的需求分析、架构设计和功能设计，总结了金融 IC 卡的实现成果、尚存在问题和发展前景，解决了金融 IC 卡运用平台建设的迫切需要，也为下一步功能拓展和深入运用打下基础。

关键词：金融 IC 卡；行业应用；统一建模语言

Abstract

Financial IC card is a product of the financial information. With the IC card technology matures and the financial industry-standard specification, the IC card security, convenience, multi-application has been widely recognized, the rapid development of a variety of domestic and foreign IC card application, docking as the financial service industry needs a realistic and necessary requirements, technology research and application of financial IC card system has also become an inevitable trend.

In the face of pressing industry pressure, strong market demand, fierce industry competition, Commercial banks develop the financial IC card industry Application platform. Based on a commercial bank financial IC card information systems development projects, by way of the system requirements analysis, system architecture design and system design, This dissertation is completed design of financial IC card industry applied research and design.

The project is based on the Tuxedo development, using an Oracle database, using the Unified Modeling Language (UML) for requirements analysis and design description language, the use of top-down, layers of refinement, hierarchical design, standardized interface to set aside technical redundancy to facilitate the expand. The front terminal management, IC card management, electronic wallet, offline consumer, the date of the final accounting treatment, reports, statistics, and key security management functions.

The system standardization the excuse and application process, full integration of the existing IC card business of the bank, better way to solve the existing systems of the bank, Provide strong support for the transition from magnetic stripe cards to the IC card bank card protection, at the same time provide a solid foundation for financial IC card-based industry application development.

This dissertation from the domestic and international financial IC card development use trends and bank card development status, improve card security and to meet the financial IC card industry application as a starting point, Around the commercial bank financial IC card project, discusses the needs analysis, architecture design and functional design, achieve results, there are still problems and development prospects, solve the financial IC card platform construction,and lay the

foundation for functional expansion and in-depth use.

Key Words: Financial IC Card; Industry Applications; UML

目 录

Contents

第一章 引 言

1970 年，法国人罗兰德·莫瑞诺（Roland Moreno）第一次将可进行编程设置的 IC（ Integrated Circuit）芯片放于卡片中，使卡片具有更多的功能。这样就诞生了世界上第一张 IC 卡。它将一个集成电路芯片镶嵌于塑料基片中，封装成卡的形式，其外形与覆盖磁条的磁卡相似。它一出现，就以其超小的体积、先进的集成电路芯片技术以及特殊的保密措施和无法被译及仿造的特点受到普遍欢迎。IC 卡的概念是 70 年代初提出来的，法国布尔(BULL)公司于 1976 年首先创造出 IC 卡产品，并将这项技术应用到金融、交通、医疗、身份证明等多个行业，它将微电子技术和计算机技术结合在一起，提高了人们生活和工作的现代化程度。IC 卡芯片具有写入数据和存储数据的能力，IC 卡存储器中的内容根据需要可以有条件地供外部读取和供内部信息处理和判定之用。

由于 IC 卡具有的巨大的技术、应用优势，我国金融和非金融部门都已认识到发展 IC 卡产业对加速我国国民经济信息化的重大作用，并与国外有关公司合作，引进制卡、读卡设备及应用的先进技术，成立有关集团、公司，以加速我国 IC 卡的应用。

以 IC 卡为载体的电子货币在百姓生活领域的应用方兴未艾，与磁条卡比较，IC 卡具有安全性好、数据存储容量大、使用方便（支持脱机交易）的特点，是理想的新一代支付工具,主要应用在交通、医疗、加油、小额购物等对快捷方便性要求高且与老百姓日常生活息息相关的领域。发行 IC 卡，对发卡银行来说，可以丰富业务品种，增强市场竞争力，取得无息存款的沉淀；对用卡商户来说，可以提高信息资源的管理能力，提高支付效率、提升营业额；对持卡人来说，可以享受小额支付的便利，同时，可以享有银行的积分奖励等优惠增值服务。鉴于 IC 卡支付的以上特点，IC 卡的应用具有良好的发展前景[1]。

1.1 项目背景

近几年来，国内外 IC 卡技术和应用发展迅猛。在国内，电信、交通、社保、石化等行业纷纷推广使用了 IC 卡技术，这对于加强政府的管理、减少现金使用、推进行业信息化等起到了积极作用。在国外，1998 年，国际银行卡公司出于防范银行卡交易欺诈风险及提升金融支付工具附加功能的考虑，制定了银行卡芯片化计划——EMV（Europay,MasterCard,Visa 公司的缩写）迁移计划，在全球推广

银行 IC 卡应用。2000 年又颁布了新版的 EMV 标准及风险转移政策（即将目前伪卡欺诈风险主要由发卡行承担的惯例，改为由发卡行、收单行中未采取 EMV 迁移的一方承担）和相关鼓励实施政策。

2010 年，随着金融 IC 卡在宁波等地的试点成功，以《中国金融集成电路（IC）卡规范》（2010 年版）的正式发布为标志，传统银行卡功能都能在金融 IC 卡上实现。央行制订了银联标准 PBOC2.0 芯片卡(IC 卡)的总体目标和具体发行时间表，5 年之内中国境内将全面发行和受理金融 IC 卡。央行 2012 年 7 月 19 日宣布，从 2013 年 1 月 1 日起，全国性商业银行均要发行金融 IC 卡。截至 2012 年上半年，全国已累计发行金融 IC 卡 4500 多万张，自 2015 年 1 月 1 日起，所有新发行的银行卡应为金融 IC 卡。

随着 IC 卡应用深入到银行、电信、社保、智能交通、工商税务、公共事业、加油、烟草等多个应用领域。IC 卡应用与金融系统的服务对接成为一种现实的和必然的要求。银行以市场为导向，为客户提供快捷方便和优质的服务，加之近期克隆卡泛滥，提高银行卡的安全性是一个不容回避的课题，因此金融 IC 卡系统的技术研究和应用也成为一种必然趋势。

1.2 国内外研究现状

早在 10 年前，国际上就已经开始银行卡从磁条卡向芯片卡(金融 IC 卡)迁移，主要动力是防范伪卡欺诈和实施多应用，目前全球已有超过 10 亿张银行卡采用金融 IC 卡标准，在使用这一标准的国家和地区伪卡欺诈率大幅下降。与此同时，我国银行卡伪卡欺诈正在呈上升趋势，引起社会的高度关注。

为适应全球银行卡芯片化迁移进程，提高我国银行卡风险防控能力，拓展银行卡在公共服务领域的应用，实现“一卡多用”和“一卡通用”，充分利用金融 IC 卡的安全、便捷、多应用优势，我国加了快金融 IC 卡的标准制定。

2005 年我国正式颁布《中国金融集成电路(IC)卡规范(V2.0)》，业内简称 PBOC2.0 规范 2005 版。2008 年组织开展了宁波等城市的金融 IC 卡多应用试点，深入、系统研究了金融 IC 卡在公共服务领域的应用前景，试点的成功进一步验证了 PBOC2.0 的标准和相关政策。2010 年人民银行，在总结试点经验的基础上，颁布《中国金融集成电路(IC)卡规范》(2010 年版)，标志着中国金融 IC 卡应用进入新的历史发展阶段。

历经 10 年的努力，人民银行组织完成了金融 IC 卡基础设施建设，已经建立

比较完善的标准规范、密钥体系、全国性交易转接和清算平台、一卡多用的业务模式，既能满足传统的支付应用，也能实现身份标识、信息记录等公共服务功能，具备了有效衔接各个部门、各项产品、各类渠道的能力。同时不断推进行业合作，推动各商业银行开始发行金融 IC 卡。

一系列的工作为全面推广金融 IC 卡提供了必要的制度和物质条件准备，在此基础上，2011 年 3 月 15 日，人民银行颁布《中国人民银行关于推进金融 IC 卡应用工作的意见》，全面启动银行磁条卡向 IC 卡迁移工作[2]。

1.3 本文的主要内容及章节安排

本文主要从金融 IC 卡的设计目标、金融 IC 卡系统结构及功能等方面，从银行发行和管理金融 IC 卡方面入手进行了详细的阐述。并以金融 IC 卡为例，从系统设计、系统架构、安全体系、业务流程等方面进行了详细的研究与设计。

本文共分为六章。

第一章为引言，简要介绍了金融 IC 卡的特性、国家标准和现行政策、在国内外推广和运用现状进行分析。

第二章介绍银行卡现状及金融 IC 卡设计目标，行外部市场环境和内部业务发展动力出发，分析金融 IC 卡推广应用的必要性。可行性，提出系统设计目标是建立一个统一、开放的 IC 卡处理平台和网络应用环境。

第三章介绍需求分析，在对业务、性能、接口等需求进行详细分析基础上，对金融 IC 卡系统目标提出完整、准确的具体要求，为下一步金融 IC 卡系统构架设计、程序结构、数据结构做出了初始定义。

第四章系统架构设计主要阐述了金融 IC 卡的系统设计规范、通过对系统的总体框架、应用架构、网络构架、安全构架、接口规范详细介绍，展示了系统设计的整体框架。

第五章详细阐明了系统的设计结构及行业应用的实现，并对核心的几个业务单元的具体设计进行具体描述。

第六章是结束语，对整个项目的分析设计过程进行了总结，并对下一步工作进行展，存在问题和需改进地方进行展望。

第二章 银行卡现状分析

我国目前银行卡市场中，以传统磁条卡占据主要市场份额，各家商业银行按人行部署饼根据市场需求，逐步推进金融 IC 卡发卡。目前各主要银行均已推出各自金融 IC 卡。

2.1 银行卡现状分析

2.1.1 银行卡数据安全性

磁条卡以液体磁性材料或磁条为信息载体，信息读写相对简单容易，使用方便，成本低，但信息存储量小、磁条信息易泄露或伪造、保密性差，从而需要计算机网络或中央数据库的支持。传统的磁条银行卡在经历多年的发展中，为银行卡业务的发展壮大发挥了重要作用，也极大地方便了广大人民群众的金融活动。随着银行卡的普及，传统的金融磁条卡由于其结构简单，存储容量小，安全保密性差，读写设备复杂且维护费用高，银行卡面临的风险形势日益严峻，银行卡诈骗等风险案件时有发生，作为七、八十年代技术水平的产品已风光不再，面临淘汰。

金融 IC 卡的出现，极大地消除了这些安全隐患，为全面代替磁条卡，创造了有利条件。金融 IC 卡是由商业银行（信用社）或支付机构发行的，采用集成电路技术， 遵循国家金融行业标准，具有消费信用、转账结算、现金存取全部或部分金融功能，可以具有其他商业服务和社会管理功能的金融工具。金融 IC 卡又称为芯片银行卡，是以芯片作为介质的银行卡。与传统的磁条卡相比，金融 IC 卡具有安全性更高、功能更强大等优势。芯片卡容量大，可以存储密钥、数字证书、指纹等信息，能够同时处理多种功能，为持卡人提供一卡多用的便利。

近段时间，全国各地连续发生 ATM 机加装复制器事件，不法分子只需要花几千元钱就能买到一个‘伪卡’的磁条复制器，通过复制器获得磁卡信息，制作“伪卡”，窃取卡内的资金。云南省不久前就发生了“伪卡”窃取现金的事件，不法份子通过“伪卡”窃取客户资金 75 万元。

金融 IC 卡的推出正是应对这种安全威胁最有力的武器。与传统的磁条卡相比，新型金融 IC 卡最大的特点是“安全”，它采用 CPU 芯片，具有独立运算、加解密和储存能力，其复制难度较磁条卡大，具有很强的安全认证机制，极大降

低伪卡欺诈风险，是目前最具安全性的银行卡。安全系数非常高的 IC 银行卡推出后，对银行和客户来说会是一个双赢。

金融 IC 卡全面推广后，‘伪卡’将会被取缔，这种带有金融支付功能的 IC 卡目前还没有破解的先例，随之而来的是客户银行卡安全性的极大提高。今后，我国银行卡将逐步由磁条卡向 IC 卡方向转变———IC 卡容量大,防伪性能更强，是应对目前银行卡犯罪最有效的办法之一。从 EMV 迁移的路径看，最早在银行卡欺诈风险较为集中的西欧地区开展，然后依次向欺诈风险较低的地区发展如亚太区、拉美区和中欧、非洲、中东区等地区延伸，这反映了各国和地区开展 EMV 迁移的初衷是为了降低伪卡欺诈，尤其在最早开展迁移的法国、英国等国家最为明显。目前在欧美等发达国家，磁条卡已经很少使用，人们的银行卡大多是 IC 卡，它采用了目前世界上最先进的密钥管理标准，是安全系数最高的银行卡。

金融 IC 卡与银行磁条卡在安全性、容量、成本、通讯网络、业务处理等方面有显著区别，如表 1-1 所示。

表 1-1：IC 卡与磁条卡性能比较

性 能	IC 卡	磁条卡
安 全 性	无法复制，数据均有读写保护，安全性高	卡中信息容易复制与读写,安全性低
容 量	存储量大、可记录交易明细，可以存放多种金融和行业及个人信息	容量小、无法存储交易信息和其他有用信息
成 本	制作成本高，单张价格 10 元以上	制作成本低,单张价格 1 元以上
通讯网络	对通讯要求不高，可以实现脱机操作	对网络要求高,只可联网工作
业务处理	可以把多种业务综合在一张 IC 卡内进行处理	不可以
其 它	CPU 卡有运算处理能力	无处理能力